DATATILSYNET

19 August 2026

The Danish Data Protection Agency concludes its investigation into the Rejsekort app

The Danish Data Protection Agency has now concluded its investigation into the Rejsekort app. Following a comprehensive assessment, the Agency finds that there are not fully sufficient grounds to express criticism of Rejsekort in the two areas on which the investigation has focused.

Summary

The Danish Data Protection Agency has investigated Rejsekort & Rejseplan A/S's processing of personal data in the Rejsekort app and, in the course of this, has obtained a number of statements from the company regarding the app's design and functionality.
The case has been considered by the Data Council.

Data minimisation and data protection by design

The Rejsekort app uses the GPS on the user's phone to record the user's location during their journey. The information is used, amongst other things, to map the journey, calculate the correct fare and allocate ticket revenue amongst the various transport operators.

Information about where a specific person is at a specific time constitutes personal data under data protection regulations.

– Information about where we are and where we are going can reveal a great deal about our private lives. It is therefore important that controllers who collect location data on citizens or customers focus on limiting the collection to what is necessary. That is why we launched an investigation into the Rejsekort app, says Morten Gjermundbo, Head of Division at the Danish Data Protection Agency.

The Danish Data Protection Agency initially raised a number of different questions regarding the Rejsekort app's processing of personal data. The investigation has since focused on two key questions:

- whether the collection of location data complies with the principle of data minimisation, and
- whether the app's design complies with the principle of data protection by design.

Following an overall assessment, the Danish Data Protection Agency now finds that there are not fully sufficient grounds to express criticism of the Rejsekort app in relation to these two issues.

The Danish Data Protection Agency's decision concerns the app's design and functionality in relation to the principles of data minimisation and data protection by design. The decision therefore does not address the app's compliance with data protection rules in general.

GPS tracking after the journey has ended

Once a user has checked in on the Rejsekort app, the app continuously collects information about the user's location during the journey. However, if the user does not check out when the journey ends, the collection of data may continue even after the user has left the public transport. In that case, personal data will be collected without any connection to the service that Rejsekort is required to provide.

This collection of personal data could potentially include sensitive information – for example, if, after their journey, the user visits a church, receives medical treatment or visits their trade union.

An overall assessment

In its overall assessment, the Danish Data Protection Agency has taken into account a number of factors that argue both for and against the Rejsekort app being in compliance with the rules. Among other things, the Danish Data Protection Agency has taken into account that, according to Rejsekort, only a small proportion of users forget or fail to check out. At the same time, the Danish Data Protection Agency has noted that Rejsekort is a nationwide system aimed at the entire population.

The Danish Data Protection Agency has also emphasised that Rejsekort has implemented a number of measures to limit the risk of unnecessary collection of location data. For example, Rejsekort has produced guidance material on the use of the app and built in a number of assistance features. These include warnings about check-out, the option to activate the 'smart check-out' function, and a mandatory automatic check-out for inactive journeys once a day.

However, the Danish Data Protection Agency has also emphasised that several of these support features require users to actively opt in. Finally, it has been significant that users are obliged to check out once their journey has ended.

Following a thorough, comprehensive assessment of the arguments for and against, the Danish Data Protection Agency has now concluded that there are not fully sufficient grounds to express criticism of the Rejsekort app.

Fundamental issues were discussed at European level

The case has raised general questions about how the rules on data minimisation and data protection by design should be interpreted in relation to an app solution such as the Rejsekort app. As the technical solution behind the app is also used for ticketing systems in other European countries, the Danish Data Protection Agency decided in June 2025 to consult other European data protection authorities on the key legal issues.

However, the feedback did not provide sufficient clarity to establish a uniform approach. The Danish Data Protection Agency therefore took steps to refer the questions to the European Data Protection Board (EDPB) for a formal opinion. The questions were discussed at working group level within the EDPB in April 2026.

Following discussions at European level, however, there was not full support for the view that the questions were suitable for an opinion from the EDPB. The Danish Data Protection Agency therefore decided – following further discussions within the Data Council – not to proceed with the request to the EDPB and instead to make a decision on the basis of the available information.
With this decision, the Danish Data Protection Agency concludes its investigation into the Rejsekort app and will take no further action in the matter.

Decision

1. Introduction and conclusion
1.1. Introductory remarks

The Danish Data Protection Agency has now completed its investigation into Rejsekort & Rejseplan A/S' (hereinafter referred to as "Rejsekort") digital travel card solution, the "Rejsekort app".

The Rejsekort app works by allowing users – instead of carrying a physical travel card – to download the company's app onto their mobile phone. Using the mobile phone's GPS tracking, Rejsekort can map the start and end points of each individual journey by public transport and thereby, amongst other things, determine the correct fare for the journey. The app replaces the old plastic travel card.

On Rejsekort's initiative, prior to the Rejsekort app being rolled out to the general public, an informal meeting was held on 15 April 2024 between Rejsekort and the Danish Data Protection Agency's secretariat, during which the Danish Data Protection Agency, as part of its general duty to provide guidance, highlighted a number of general IT-related and data protection issues that Rejsekort might wish to consider prior to the roll-out of the app.

By letter dated 30 April 2024 to Rejsekort, the Danish Data Protection Agency formally initiated its investigation into the matter. On the basis of Rejsekort's response, the Danish Data Protection Agency, by letters dated 27 June 2024, 6 February and 28 April 2025, requested explanations regarding further matters concerning the Rejsekort app.

On 27 May 2025, at Rejsekort's request, a further meeting was held regarding the case.

In connection with its investigation of the case, the Danish Data Protection Agency has asked Rejsekort to provide explanations on a number of different matters, including, amongst other things, the following topics:

- data minimisation
- data protection by design
- legal basis
- considerations regarding technical solutions other than the collection of location data
- duty to provide information
- pseudonymisation/anonymisation of personal data collected
- Deletion/storage limitation

The Danish Data Protection Agency's investigation has focused on the issue of data minimisation and data protection by design.

When using the old Rejsekort (the plastic card), users would occasionally forget to check out. A key issue in this case has been the data collection that takes place if a user of the Rejsekort

app similarly forgets to check out and moves away from the public transport system. Once the journey has ended, the user's subsequent movements are irrelevant to the service that Rejsekort is required to provide.

In light of this, the Danish Data Protection Agency's investigation has primarily focused on the following two issues:

1) Whether the collection of personal data in the form of users' GPS location after the end of a journey contravenes the data minimisation principle under data protection law, as set out in Article 5(1)(c) of the General Data Protection Regulation, and

2) whether an app designed or developed in the manner described above contravenes the principle of data protection by design, as set out in Article 25 of the General Data Protection Regulation.

The Danish Data Protection Agency has referred these two key and general legal questions to the other European supervisory authorities, and has also recently taken steps to refer the questions to the European Data Protection Board (hereinafter referred to as 'EDPB', which is an abbreviation of the Board's English name, European Data Protection Board) with a view to obtaining a formal opinion from the Board on how these provisions of the Regulation should be interpreted in relation to an app that functions in the same way as the 'Rejsekort app'.

In light of the feedback received by the Danish Data Protection Agency in this regard, the Agency has decided not to request an opinion from the EDPB, and has instead now reached its own decision on the matter.

The case has been considered by the Data Council, which, at a series of meetings, has taken decisions on the handling of the case and – now – on the outcome of the case.

1.2. The Danish Data Protection Agency's conclusion

Based on an overall assessment of the available information, the Danish Data Protection Agency concludes that there are not fully sufficient grounds to express criticism of Rejsekort & Rejseplan A/S in connection with the company's launch of the Rejsekort app.

A more detailed review of the case follows below. The grounds for the Danish Data Protection Agency's decision are set out in section 5.

2. Legal basis

2.1. The Public Transport Companies Act, etc.

It follows from the Public Transport Companies Act that the public limited company Rejsekort & Rejseplan A/S must provide an electronic journey planning system and an electronic travel card system for ticketing and payment, etc., and that the company must furthermore integrate the electronic journey planning and travel card systems into a single mobility service. The Act was most recently published as Consolidated Act No. 1041 of 17 September 2024.

The relevant provisions (which were inserted by Act No. 206 of 5 March 2019) read as follows:

> **"Section 27.** The transport companies, Bornholm Regional Municipality, Metroselskabet I/S and DSB shall, within a public limited company named Rejsekort & Rejseplan A/S, operate and develop an electronic journey planning system providing information on journey times, journey planning and fares, etc., and an electronic travel card system for ticketing and payment, etc.
> Paragraph 2. (…)
> Paragraph 3. (…)
> Paragraph 4. (…)
> Paragraph 5. (…)
> Paragraph 6. (…)
> Paragraph 7. (…)

Paragraph 8. (…)

Paragraph 9. Rejsekort & Rejseplan A/S shall draw up a business plan which must include a strategy for

1) integrating the electronic journey planner and travel card system into a single mobility service,

2) creating the best possible framework for third-party access to the company's services, and

3) creating the best possible conditions for third-party resale of tickets.

Paragraph 10. Rejsekort & Rejseplan A/S must submit a report to the Minister for Transport once a year, in which the company sets out the implementation of the mandatory points in its business plan, cf. paragraph 9, nos. 1–3.

Paragraph 11. The Minister for Transport may lay down further rules concerning Rejsekort & Rejseplan A/S's operation and development of the journey planner and travel card system, including the financing of such operation and development, the prioritisation of development initiatives and objective conditions for connection to the journey planner and travel card system."

The authorisation in section 27(11) of the Act does not appear to have been utilised.

The general explanatory notes to the Bill (Bill No. L129 of 19 December 2018, page 4) state, amongst other things, the following:

"1. Introduction

(…)

By making use of the opportunities offered by digitalisation, it will become easier to travel on public transport; for example, journeys will be able to be planned, booked and paid for in a single app. In this way, passengers' choices can be increased, and the integration of the various transport services can contribute to a more coherent transport system as well as increased and more efficient mobility in society.

(…)

Whether travellers prefer the fastest, the most comfortable or the cheapest journey, digital mobility services can make it easier to find, plan and pay for their journey. Mobility services improve conditions for travellers and increase passengers' mobility options and freedom of choice.

(…)

Public transport operators are already moving in the right direction, and through the development and operation of the journey planner and travel card to date, they have succeeded in establishing a strong position for public transport in Denmark and a solid digital foundation for further development for the benefit of consumers. However, digital developments have made it possible to achieve even more in this area, both for individual travellers and for mobility in society as a whole. The aim of the bill is therefore to support the positive momentum already underway in the sector by promoting the further development of the services' functions, so that in the long term they can operate as a single, integrated service.

(…) The aim is to ensure a targeted and joint strategy for a unified digital service and a coordinated prioritisation of development initiatives for both products. By consolidating these tasks, the aim is to make better use of knowledge, skills and managerial capacity, whilst ensuring a higher degree of synergy and consistency in the decisions taken. (…) It is also proposed that public transport operators should make selected static and dynamic transport data available to third parties free of charge. Transport data primarily refers to information relating to the means of transport in question, including, amongst other things, details regarding the capacity and location of such means of transport, which enables the development of digital mobility services where users can search for, plan, book and pay for their entire journey.

The Bill therefore does not provide for the sharing of personal data, including sensitive personal data, travel patterns or the traveller's location, etc. Furthermore, both the publicly funded mobility service and any new, privately initiated mobility services will – like other businesses – be subject to the rules laid down in the General Data Protection Regulation and the Data Protection Act.

(…)

2. Key points of the Bill

(…)

2.4. A joint company for the journey planner and travel card system
(…)

2.4.2. The Ministry of Transport, Building and Housing's considerations and the proposed scheme
(…)

It is the Ministry's view that there is great potential in linking the further development of the journey planner and the travel card in order, in the long term, to promote initiatives where journey planning, booking, payment and ticketing for various forms of transport services are integrated into a single digital mobility service, accessible nationwide whenever the need arises.

A key long-term objective is therefore to establish a service that, as far as possible, combines the current products and services of the Rejsekort and the travel planner, as well as future products and services that are under development.

(…)

However, it is crucial for user satisfaction with the Rejseplan and Rejsekort systems that ongoing consideration is given to whether and how the systems can be developed in terms of both form and content, including how the Rejsekort – in line with the rest of society – should move towards increased digitalisation.

(…)

Furthermore, Rejsekort & Rejseplan A/S is required to draw up a business plan, which the company must submit once a year to the Minister for Transport, Building and Housing.

The business plan must contain a strategy and timetable for the implementation of the company's tasks, and the plan must address the initiatives set out in the Minister for Transport, Building and Housing's proposal from September 2018 on simplifying public transport, including how the company's functions can most appropriately be consolidated into a single mobility service, where users can search for a suitable journey based on their preferences, book the journey and, finally, pay for it. (…)

2.5. Functions and use of the journey planner and travel card system
(…)

2.5.2. The Ministry of Transport, Building and Housing's considerations and the proposed scheme
(…)

The proposal therefore aims to support the further development of the journey planning system's functions with a view to providing, in conjunction with the travel card system's functions, a unified digital mobility service where journey planning, booking, ticketing and payment can be accessed via a single, integrated service across public and private modes of transport and providers. (…)

2.8. Data protection of personal data
(…)

Notwithstanding this, the future company Rejsekort & Rejseplan A/S will, to a large extent, process personal data in connection with its administration of, amongst other things, the Rejsekort, as is already the case today for the two existing companies. For example, Rejsekort A/S already processes personal data in connection with the ordering and use of Rejsekort, including CPR numbers in connection with the ordering and administration of personal Rejsekort.

(…)"

The explanatory notes to the Bill (p. 19) state, amongst other things, the following:

"Re Section 1
(…)

Re No. 6

(…)

The proposed provision enshrines in law that the parties must cooperate to operate and develop a joint journey planner and travel card system within a single company. The journey planner and travel card have become widely accepted by passengers on public transport services across the country, and it is expected that by bringing these activities together within a single company, the systems can be better maintained and developed in line with technological advances.

The term 'journey planning system' means that public transport operators must offer a journey planning system that is, as a minimum, equivalent to the electronic journey planning system currently operated by Rejseplan A/S on behalf of public transport operators in Denmark.

The term 'travel card system' means that public transport operators must offer a ticketing system that is, at a minimum, equivalent to the electronic travel card system currently operated by Rejsekort A/S on behalf of public transport operators in Denmark.

(…)"

As stated in section 2.4.2 of the general explanatory notes to the Bill, Rejsekort must draw up a business plan which, amongst other things, must address the initiatives set out in the Minister for Transport, Building and Housing's proposal from September 2018 on easier public transport1 .

Under the heading 'Easier public transport', Rejsekort's draft business plan sets out the following initiatives:

"Initiatives to promote digital mobility services

- Efforts should be made to consolidate the functions of Rejseplanen and Rejsekort into a single digital mobility service under one company with a single board of directors.
- Private and sharing economy transport providers must have access to the joint digital mobility service.
- Public transport operators must be required to share transport data and to accept the resale of tickets, so that private transport operators can establish more digital mobility services."

Under the heading 'Further development of existing digital mobility services', the proposal contains the following initiatives:

"Initiatives

- Efforts must be made to consolidate the functions of Rejseplanen and Rejsekortet into a single digital mobility service.
- Cooperation on the operation of Rejseplanen and Rejsekortet and the development of the digital mobility service will be consolidated into a single company with a single joint board of directors.
- The State will share responsibility by sitting on the joint board."

Under the heading 'More new digital mobility services', the proposal contains the following initiatives:

"Initiatives

- Private and sharing economy transport providers must have access to Rejseplanen and Rejsekortet's joint digital mobility service, so that passengers have more choice.
- Public transport services must be required to share transport data and to accept the resale of tickets, so that it becomes possible to establish more private digital mobility services.
- Standardised ticketing formats must be established to enable the validation of new ticket types based on public sector standards."

1 https://www.trm.dk/media/k0ldhxxu/nemmere-kollektiv-trafik-endelig-til-web-final-a.pdf.

2.2. Article 5 of the General Data Protection Regulation

Article 5(1) of the General Data Protection Regulation sets out a number of general principles governing the processing of personal data. The provision reads as follows:

> "Personal data shall:
> (a) be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
> (b) be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (…) ('purpose limitation')
> (c) be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
> (d) be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay ('accuracy')
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Recital 39 of the General Data Protection Regulation states the following regarding the principle of data minimisation:

> "(39) […] Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This requires, in particular, ensuring that the period of storage is no longer than strictly necessary. Personal data should only be processed if the purpose of the processing cannot reasonably be achieved by other means. […]"

In the Ministry of Justice's Report No. 1565/2017 on the General Data Protection Regulation – and the legal framework for Danish legislation, pages 87–88, the following is stated regarding the previously applicable and almost identical provision in Section 5(3) of the Personal Data Act, which implemented Article 6(1)(c) of the former Data Protection Directive (Directive 95/46/EC):

> "It follows from Section 5(3) of the Data Protection Act that data being processed must be relevant and adequate and must not go beyond what is required to fulfil the purposes for which the data are collected and the purposes for which the data are subsequently processed.
>
> It is stated in the explanatory notes to the Data Protection Act that the terms 'relevant' and 'adequate' information refer to the fact that the nature of the information must correspond to the purpose intended by the processing. The provision further stipulates that the controller's processing of information is subject to the principle of proportionality."

It is also apparent from page 97 of the report that, based on a literal interpretation of Section 5(3) of the Personal Data Act, and Article 5(1)(c) of the General Data Protection Regulation, no different substantive meaning is intended for Article 5(1)(c) than that which applied under the Personal Data Act.

The 'General Data Protection Regulation and the Data Protection Act with Commentary' (2, page 340) states the following regarding Article 5(1)(c) of the General Data Protection Regulation:

> "The processing of data must not go beyond what is necessary to fulfil the purposes for which the controller is authorised to process the data, i.e. the controller's processing of personal data is subject to the principle of proportionality."

2.3. Article 25 of the General Data Protection Regulation

Article 25 of the General Data Protection Regulation lays down rules on 'data protection by design and data protection by default'. Paragraphs 1 and 2 of that provision read as follows:

> **"1.** Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> **2.** The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

Recital 78 of the General Data Protection Regulation further states:

> "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."

Report No. 1565/2017 on the General Data Protection Regulation – and the legal framework for Danish legislation, page 417, states the following regarding Article 25(1) of the Regulation:

> "Article 25(1) of the Regulation must be understood as imposing a *duty of consideration* and a *duty of action* on the controller to incorporate, as early as the preparatory phase, the relevant measures to ensure compliance with the General Data Protection Regulation. […]
>
> It should be noted in this regard that Article 25(1) of the Regulation reflects a risk-based approach to data protection, and the provision sets out only very general

2 The General Data Protection Regulation and the Data Protection Act with commentary, Kristian Korfits Nielsen and Anders Lotterup, 2nd edition, 2025.

> guidelines as to the types of measures it is intended to cover. This means that the controller is afforded considerable discretion, within which they are free to assess and determine which specific measures should be implemented to comply with the provision.
>
> Article 25(1) must be understood as imposing a duty on the controller to incorporate measures that specifically promote the effective implementation of the data protection principles set out in Article 5 of the Regulation and its other provisions.
>
> The controller must therefore consider and address how data protection in general – that is, all the provisions of the Regulation – can be complied with through specific measures in *the design* of IT systems, such as their technical architecture and user interface, as well as in *the organisation* of the controller's operations."

Regarding Article 25(2) of the Regulation, the following is stated on page 420 et seq. of the report:

> "Unlike the provision in Article 25(1), which concerns the design phase itself, Article 25(2) is understood to impose a duty on the controller to ensure that, for example, when a software programme, an online service, an IT system or similar is used to process personal data, the settings available in the system, etc., must by default be configured in a way that supports the provision's requirements regarding, amongst other things, the purpose-specific processing of personal data.
>
> This requirement must, for example, mean that the first time a service – such as an online service, an app or a piece of software – is made available to a given user or employee, the relevant settings relating to the processing of personal data in connection with the use of the service must, in accordance with the data minimisation principle in Article 5(1)(c), by default entail the minimum possible sharing of personal data.
>
> The requirement in Article 25(2) may thus be regarded as a 'supplement' to the requirement for data protection by design in Article 25(1), in that paragraph 1 may specifically entail that a system is designed with specific data protection-enhancing settings built in, and the provision in Article 25(2) thus requires the controller, for example, to make the setting that most restricts the purpose of the system the default setting. […]"

The EDPB's guidelines on data protection by design and by default[3] state, amongst other things, the following regarding data protection by design and by default:

> "(19) In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology** that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape.
>
> (…)
>
> (49) Controllers should consider both the volume of personal data, as well as thetypes, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/or less detailed information about data subjects. In any case, the default setting shall not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data isn't needed because less granular data is sufficient, then any surplus personal data shall not be collected.
>
> (…)

3 Guidelines 4/2019 on Article 25, data protection by design and data protection by default, version 2.0, adopted on 20 October 2020.

(74) Controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all37. Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle. This is also consistent with Article 11.

(…)

(76) Key design and default data minimisation elements may include:

(…)

- Limitation – Limit the amount of personal data collected to what is necessary for the purpose.

(…)"

3. Statement of the case

3.1. Basic information on how the Rejsekort app works

The Rejsekort app has several different functions, including journey planning, ticket booking and purchase, and it can also be used as proof of a valid travel authorisation during ticket inspections.

When travelling using the app, the traveller's physical location is tracked via the phone's GPS. The purpose of this tracking is, amongst other things, to ensure that a correct and valid ticket is issued, to calculate the correct fare, and to ensure the correct allocation of ticket revenue to the various transport operators whose services may have been used during the journey.

The user determines the start and end times for GPS tracking by 'swiping' on their phone to check in and out of the app, at which point tracking begins and ends accordingly.

3.2. The Danish Data Protection Agency's questions to Rejsekort & Rejseplan A/S

On 30 April 2024, the Danish Data Protection Agency requested that Rejsekort specify which personal data is processed in the Rejsekort app and explain the considerations the company had made in relation to the principle of data minimisation and the design of the app.

On 27 June 2024, the Danish Data Protection Agency requested a supplementary statement from Rejsekort on the extent to which the collection of location data is necessary to achieve the purpose of the processing, and to what extent the underlying agreement on the distribution of ticket revenue to the various public transport providers, combined with a desire to offer a good user experience, can collectively be regarded as legitimate grounds for the design of the technical solution, including the collection of location data.

In this context, the Danish Data Protection Agency also asked Rejsekort to comment on whether the collection of personal data in the Rejsekortapp leads to excessive data processing that is not in accordance with, amongst other things, the principle of data minimisation in Article 5(1)(c) of the General Data Protection Regulation and the obligation to ensure data protection by design and by default under Article 25.

On 6 February 2025, the Danish Data Protection Agency requested a further supplementary opinion from Rejsekort on the possibilities of making a number of 'check-out' solutions in the Rejsekort app mandatory for users, and on the potential consequences the changes might have for Rejsekort and users respectively.

In the same context, the Danish Data Protection Agency asked Rejsekort for an update on the expected anonymous alternative to the Rejsekort app, which the company had informed the Agency was under development in a previous opinion.

Finally, on 28 April 2025, the Danish Data Protection Agency asked Rejsekort to comment on whether the Rejsekort app could have been designed differently, based on a number of outlined fundamental principles, so that the app would still meet the defined technical requirements and user-friendliness criteria, etc., but with a less intensive collection of user data, including location data.

3.3. Information provided by Rejsekort & Rejseplan A/S to the Danish Data Protection Agency

Rejsekort has stated that the Rejsekort app is provided by the Swiss company FAIRTIQ as a 'Software as a Service' solution, hosted in a cloud environment by Amazon Web Services. Regarding the choice of solution, Rejsekort has stated that it was crucial for the company to find a tried-and-tested standard system, so that there would be only a limited need for customisation of the solution.

To use the Rejsekort app, you must create a profile and, in doing so, provide a range of details, including:

- first name and surname,
- email address,
- telephone number,
- date of birth, and
- payment details.

Information is then collected regarding:

- the user's customer number,
- the user's ticket settings (including customer type and, where applicable, discount tier)
- the user's IP address and
- the ID number of the mobile device on which the profile was created.

When using the Rejsekort app, information is collected on:

- the user's location data (GPS coordinates with a timestamp from the user's phone),
- activity data (exercise and fitness data from the user's phone) and
- beacon data (Bluetooth signals from the user's phone, collected, for example, at stations with poor internet coverage, such as underground when travelling on the metro).

Furthermore, Rejsekort has stated that only general information about data subjects is processed in the Rejsekort app.

It has been stated that personal data is processed in the Rejsekort app for the following purposes:

1. Provision of the Rejsekort app (overarching purpose), including
a) PAYG (Pay As You Go – purchase of a valid travel ticket)
b) Customer service
c) Financial settlement between transport operators
2. Fraud detection
3. Bug fixing
4. Showing a ticket to a ticket inspector

Rejsekort has also stated that, for the Rejsekort app to function, it is necessary, amongst other things, to collect location data in order to map the user's journeys. This data is recorded in a personally identifiable form, as each individual user of the app pays for the journeys they actually make. The primary purpose of collecting location data is therefore to provide the user with a valid travel authorisation, to charge the correct fare and to ensure the correct distribution of ticket revenue to the providers.

Unlike the physical Rejsekort, where information is collected only 'at specific points' regarding where users check in and out, the Rejsekort app continuously collects information on the user's location throughout the journey, and in certain cases also before the journey begins and after it has ended.

Furthermore, Rejsekort has stated that if individual journeys are not recorded, it will not be possible to see which modes of transport the customer has used, when this took place, what fare the customer has paid, and how this should be allocated. In that case, it would not be possible to carry out an internal allocation of revenue from customers in accordance with the relevant agreements between the transport operators. The introduction of the Rejsekort app means that, for approximately half of all journeys, detailed data is available for each individual journey, making it possible to switch to source-based allocation in the revenue-sharing arrangement between transport operators. Source-based allocation means that ticket revenue from each individual journey is allocated on the basis of the data specific to that journey.

Rejsekort has also stated that the company has regularly conducted customer surveys with a view to ensuring customer satisfaction, including to gain an insight into what changes customers would like to see made to the physical Rejsekort. In this context, requests were identified, amongst other things, for the travel card to be digitalised on a mobile phone rather than being a physical card, for it to be possible to check in and o ly via a mobile phone rather than at a physical card reader, and to avoid having to check in again when changing modes of transport during the same journey. In developing the Rejsekort app, Rejsekort has prioritised ensuring that the app is user-friendly and, as far as possible, meets the requests that were regularly identified in user surveys.

Rejsekort has generally stated that, pursuant to Section 27 of the Transport Companies Act, the company is obliged to offer a comprehensive, digital journey planning system and travel card system for ticketing, payment, etc. Rejsekort has pointed out that the launch of the Rejsekort app is thus stipulated in the Public Transport Companies Act and that the app is operated within the framework of the Act.

Rejsekort has further stated that, when the Public Transport Companies Act and the specific provisions on a single, integrated mobility solution were adopted, the intention was to create a solution that makes it easy and accessible for customers to use public transport. The collection of location data makes it easy for customers, as it means they do not need to actively register this information themselves.

In this context, it is stated that it is Rejsekort's view that it is both envisaged by the Act on Transport Companies and objectively justified that the Rejsekortapp has been developed to ensure that users do not have to manually select a departure and arrival point from, for example, a list or search result, and that users do not have to check in and out en route when using combined modes of transport, whilst at the same time doing so in a way that does not give rise to an unacceptable level of misuse without the possibility of appropriate control. It is Rejsekort's assessment that the chosen solution, whereby the route and mode of transport are calculated using location data, meets these requirements.

According to Rejsekort, this should also be seen in the context of the company having developed an alternative solution where customers can travel anonymously as an alternative to the Rejsekort app. Rejsekort's development of apps, supplemented by this alternative solution (for those who cannot or do not wish to use an app), ensures broad and robust accessibility for all customers. This supports the view that, overall, this is a balanced solution in which customers are given a choice and retain control, including in relation to the sharing of their location data.

Rejsekort's first version of the impact assessment for the Rejsekort app states the following in the summary of the assessment:

> " One of the most significant risks across all processing activities in the Rejsekort app is the risk of a failure to implement data minimisation, including, in particular, the risk

> that more location data is collected than necessary, or that location data is retained for longer than necessary. This naturally follows from the fact that this is a technical solution based on the recording and processing of customers' movement patterns when the app is used. Before mitigating measures are implemented, the risk is assessed as medium."

Rejsekort has, in its considerations regarding the principle of data minimisation, stated, amongst other things, that the company is aware that a failure to minimise data constitutes perhaps the greatest data protection risk in solutions of this type, which are based on the recording of users' location data. This is particularly true as the collection of location data is ultimately controlled by the customer. Even though technical measures have been put in place to ensure data minimisation, it is ultimately the customer's circumstances that risk leading to more extensive data collection than necessary.

Rejsekort has further stated that, from the outset of the development project, the company has been mindful that the collection of location data must be minimised to what is necessary for the purpose. For this reason, a number of features have been incorporated into the app's design with a view to minimising the collection of location data.

This includes, amongst other things, making it clear to users within the app when location data is being collected, as well as ensuring that app users receive so-called 'check-out warnings' when the system determines that they are no longer on public transport. Users also have the option to enable the ' ' feature, which is a function within the app allowing the user to choose to receive a push notification with a countdown when the app determines that the user is no longer travelling on public transport. The 'smart check-out' feature thus sends a message stating that the user will be checked out unless they interrupt the countdown. In addition, the app includes a feature designed to ensure that, once a day, a forced check-out is carried out for all inactive journeys where the user remains checked in to the system.

Rejsekort has considered whether it is possible to make push notifications containing these so-called 'check-out warnings' mandatory for all users of the app, for example, so that the app only functions if the user allows push notifications. In this regard, it has been stated that, in Rejsekort's view, it would not strike the right balance to require all users to accept push notifications as a means of ensuring data minimisation in the event of a forgotten check-out. Such a measure would affect all users, but would only be targeted at a very limited group who forget to check out, despite the fact that, according to the terms and conditions, this is the responsibility of the individual user. Furthermore, there would be a significant risk that the Rejsekort app would be removed from app stores if push notifications were made mandatory within the app, as, in Rejsekort's view, this would contravene the requirements governing a provider's use of push notifications.

Rejsekort has explained, regarding the considerations behind making the 'smart check-out' function an optional feature in the app, that any concerns users may have about whether they continue to hold a valid travel authorisation throughout their journey have been taken into account in the decision to retain 'check-in' and 'check-out' as the default settings in the Rejsekort app. The chosen setup ensures that the user experience in both the app and on the physical card is consistent, and that users can easily understand what is expected of them as travellers. Furthermore, the 'smart check-out' function has been developed and tested by the system supplier for more than two years as part of user-oriented solutions in Switzerland, Germany and Austria. Based on this experience and following thorough discussions between Rejsekort and the supplier, the function has been configured relatively conservatively in terms of when users are automatically checked out, to prevent users from inadvertently losing their valid travel authorisation whilst on their journey.

In this context, Rejsekort has stated that, in its experience, users are good at checking out when their journey ends, and that, on average, user-initiated check-outs occur approximately 22 minutes faster than for journeys concluded via the smart check-out function.

The mandatory check-out is carried out automatically once a day – at 04:00 – for all users who are checked in via the Rejsekort app but are no longer using public transport. Rejsekort has stated that this mandatory, automatic check-out is a standard feature of the supplier's solution, and that it is a backup function intended to cover situations where users have forgotten to check out 'despite the other data-minimising measures' incorporated into the app, including check-out warnings and the Smart Check-out function.

Rejsekort has also stated that initial experience with the app shows that approximately 0.1–0.3 per cent of journeys are closed via the mandatory automatic check-out at 04:00.

Rejsekort has stated that the setting of the time at 04:00 is based on the supplier's experience from other European countries and corresponds to Rejsekort's own experience in Denmark, including many years' experience with the physical Rejsekort as a travel cardsolution, which shows that at 04:00 there are relatively few passengers on public transport. The intention behind setting this time is for Rejsekort to minimise the number of users affected whilst they are still travelling. It would be perceived as a major inconvenience by users if their valid travel authorisation were automatically deactivated by the system whilst they are still travelling, as this could lead to fines for fare evasion and a general loss of trust in the reliability of the Rejsekort app.

Rejsekort has explained in detail that it will not be technically possible to set the mandatory, automatic check-out on a completely individual basis, for example based on an individual user's typical travel patterns or personal preferences. However, the company has stated that it will be possible to reduce the ' ' period if the time limit is set for each individual journey; this would require the fare associations to agree on a standard time limit for how long a journey may last across all journeys in Denmark. At present, the maximum duration varies considerably between fare zones.

Rejsekort has stated, in general terms, that the Rejsekort app could not have been designed any other way.

4. The EU law aspects of the case

The Rejsekort app is based on technology from the Swiss supplier, FAIRTIQ AG (hereinafter 'FAIRTIQ'). This is because, in 2023, Rejsekort conducted a tender for the Rejsekort app, which was won by this company.

Rejsekort has stated that FAIRTIQ's solution is used for ticketing systems in Switzerland, Austria, Germany and France.

According to information from the Danish Data Protection Agency, none of the supervisory authorities in the countries concerned appear to have taken a position on whether the app – or app solutions designed in a similar way – complies with data protection rules.

Taking into account the provisions of the General Data Protection Regulation (GDPR) on cooperation between supervisory authorities to ensure a consistent interpretation of the rules, and because a ruling on the two key and general legal issues of data minimisation and data protection by design could have implications for similar cases in other EU countries, the Danish Data Protection Agency decided that it was most appropriate to consult the other European supervisory authorities on these legal issues.

The Danish Data Protection Agency therefore sent a request in June 2025, pursuant to Article 61(1) of the General Data Protection Regulation, for mutual assistance regarding these issues. It follows from this provision, amongst other things, that supervisory authorities shall exchange relevant information and provide mutual assistance to one another with a view to implementing and applying the General Data Protection Regulation in a consistent manner, and shall take measures to ensure effective cooperation with one another.

However, the responses did not provide sufficient clarity to establish a consistent approach to the two issues mentioned. The Danish Data Protection Agency therefore decided that it was necessary to inform the EDPB that, with reference to Article 64(2) of the General Data Protection Regulation, it intended to request a formal opinion from the EDPB on the two key legal issues.

It follows, inter alia, from Article 64(2) of the General Data Protection Regulation that a supervisory authority 'may request that any matter of general application or producing effects in more than one Member State be discussed by the European Data Protection Board with a view to an opinion (…)'.

Before a request for an opinion from the EDPB under Article 64(2) is formally submitted, the wording of the question or questions on which the supervisory authority seeks an opinion must be discussed in an expert working group under the EDPB to ensure that the questions are of such a general nature that the EDPB can issue an opinion on them.

Against this background, the following questions were discussed at working group level within the EDPB in April 2026:

- "In light of the fact that passivity/failure to manually check out can lead to intrusive GPS-tracking of data subjects outside public transport, and simultaneously bearing in mind that users have a contractual obligation to check out and have the possibility of activating various assisting features, should then the principle of data minimization in Article 5(1)(c) GDPR be interpreted in such a way that it constitutes a violation of this principle if a mobile phone app – designed to collect information on the users' locations via GPS tracking – is relying on the users to manually deactivate the tracking?

- Should it be considered compatible with the obligation of "data protection by design" to distribute an off the shelve-mobile phone app as mentioned?"

However, at working group level, there was not full support for the view that the legal questions mentioned above were suitable for the EDPB to issue an Article 64(2) opinion on them. A number of supervisory authorities were thus of the view that the Danish Data Protection Agency's questions were not sufficiently general nature, but related too specifically to a particular case.

Although the Danish Data Protection Agency does not agree with these considerations, following further discussions in the Data Council, it was decided that the Danish Data Protection Agency should not submit a request to the EDPB for an Article 64(2) opinion, and that the Danish Data Protection Agency should instead take a decision on the matter on the basis of the information available.

5. Reasons for the Danish Data Protection Agency's decision

5.1. Overall assessment

In connection with its investigation of the Rejsekort app, the Danish Data Protection Agency initially raised a number of different questions. In relation to the responses received by the Danish Data Protection Agency from Rejsekort, the Agency has primarily focused on the collection of personal data in the form of users' location data, which takes place after a journey has ended but before the user has checked out. The Danish Data Protection Agency's focus has been on whether the design of the Rejsekort app complies with the principles of data minimisation and 'data protection by design' set out in Article 5(1)(c) and Article 25 respectively.

With this decision, the Danish Data Protection Agency issues a comprehensive ruling on these two issues.

5.2. The Danish Data Protection Agency's previous practice

The Danish Data Protection Agency has issued a large number of decisions concerning the principle of data minimisation.

In case 2014-632-0081 (The Capital Region and the use of fingerprints in blood donation), the Danish Data Protection Agency found that a solution chosen by the Blood Bank at Rigshospitalet for the identification of blood donors did not comply with the data minimisation principle. The chosen system used fingerprint identification to ensure that a given blood donor was the person the system and blood bank staff expected. The Capital Region recorded images of the donors' fingerprints and not merely mathematical values calculated on the basis of these.

The Danish Data Protection Agency concluded – following referral of the case to the Data Council – that, amongst other things, the chosen solution did not comply with the data minimisation rules in force at the time under Section 5(3) of the Personal Data Act, as the chosen solution was significantly more intrusive towards the data subjects than was necessary to fulfil the purpose.

In case 2018-31-0070 (TDC and traffic and location data), TDC had, over a period of 10 months, carried out 11,366 loggings of location data relating to mobile data traffic and recorded 185 so-called MMS CDR records concerning a citizen. In general, TDC argued that it was necessary to record location data for all mobile devicesdata traffic in order to comply with the requirements of the Data Retention Order regarding the recording of location data for MMS communications, as the technical structure of TDC's mobile network did not allow for the recording of location data for MMS communications alone without simultaneously recording location data for all mobile data traffic.

The Danish Data Protection Agency found – after the case had been referred to the Data Council – that the structure of TDC's IT system could not justify non-compliance with data protection rules, and that TDC's processing of personal data, which the company had not been obliged to record under the Data Retention Order, contravened Article 5(1)(c) of the General Data Protection Regulation on data minimisation. The Danish Data Protection Agency noted that the vast majority of the information that TDC had recorded about the data subject was not necessary to comply with TDC's obligations under the Data Retention Order.

In case 2022-432-0099 (the Agency for Digitisation and the driving licence app), the Danish Data Protection Agency – also following referral to the Data Council – found that the Agency for Digitisation's processing of personal data in connection with the administration and operation of the driving licence app was in breach of Article 5(1)(c) of the General Data Protection Regulation on data minimisation. The Agency for Digitisation's driving licence app, which was a voluntary supplement to the physical driving licence, was structured in such a way that the Agency for Digitisation stored a copy of all valid Danish driving licences via an extract from the driving licence register (3.96 million citizens). The Agency for Digitisation thus processed personal data relating to a very large proportion of the Danish population who had not signed up for the digital driving licence (2.26 million citizens). The Danish Data Protection Agency emphasised, amongst other things, that the design of the app – including the extraction of information on all holders of a valid Danish driving licence from the driving licence register – was not necessary for the operation of the app, and that the chosen solution therefore failed to comply with fundamental principles. Furthermore, the Danish Data Protection Agency placed particular emphasis on the fact that waiting times or delays in creating a digital driving licence cannot, in themselves, be regarded as such a significant negative consequence for citizens as to justify the very extensive processing of personal data involved.

In case 2023-431-0013 (Dansk Retursystem and the deposit app), Dansk Retursystem had developed a deposit app that could pay out the deposit amount via direct bank transfer to users' accounts. However, in this context, not only were users' account details collected, but also information concerning, amongst other things, users' accounts, balances, loans, identity details and transaction history. The Danish Data Protection Agency found that this processing

of personal data was, amongst other things, in breach of Article 5(1)(c) and Article 25(1) of the General Data Protection Regulation, as more information about users was collected than was necessary.

In case 2024-432-0041 (DR's mandatory login on DRTV), DR had introduced a requirement to log in in order to view streaming content on DRTV. The Danish Data Protection Agency therefore investigated whether DR's processing of personal data in this context complied with data protection rules, including the legal basis requirement and the principle of data minimisation. In this regard, DR highlighted its obligation to provide modern public service to the Danish population, including online public service, and that DR's streaming content should be able to deliver a coherent and personalised user experience that met users' expectations. DR also argued, amongst other things, that a streaming service without a login and without the features available to users who log in did not constitute a contemporary service and would therefore fail to meet the obligations DR had as a public service broadcaster.

After the case had been considered by the Data Council, the Danish Data Protection Agency did not find fully sufficient grounds to conclude that DR's processing of personal data in connection with the login requirement was in breach of the legal basis requirement. The Danish Data Protection Agency noted that, pursuant to Article 6(1)(e) of the General Data Protection Regulation, in conjunction with the public service obligation as set out in the Radio and Television Broadcasting Act and in the public service contract, DR collected certain information in connection with the use of DRTV. In this connection, the Danish Data Protection Agency emphasised, amongst other things, that the scope of DR's public service obligation could not be determined unequivocally, and that such a detailed determination depended on assessments under media law, which did not fall within the core remit of the Danish Data Protection Agency's competence.

However, the Danish Data Protection Agency found that the fact that DR had organised the login process in such a way that users were, for a long time, asked to provide their name – rather than a fictitious profile name – did not comply with the principle of data minimisation, cf. Article 5(1)(c) of the General Data Protection Regulation. In this regard, DR itself had acknowledged that it was not necessary to know users' names.

5.3. The Danish Data Protection Agency's assessment

It follows from the Public Transport Companies Act that Rejsekort & Rejseplan A/S must develop an electronic journey planning system providing information on journey times, journey planning and fares, etc., and an electronic travel card system for ticketing and payment, etc. The explanatory notes to the proposed bill state, amongst other things, that "by making use of the opportunities offered by digitalisation", it will become easier for passengers to use public transport, for example because journeys will be able to be "planned, booked and paid for in a single app". It is also stated in the explanatory notes that the system must comply with data protection rules.

As Rejsekort has informed the Danish Data Protection Agency, Rejsekort noted the following, amongst other things, in its original impact assessment:

> "(…) One of the most significant risks across all processing activities in the Rejsekort app is the risk of a failure to implement data minimisation, including, in particular, the risk that more location data is collected than necessary, or that location data is retained for longer than necessary. This naturally follows from the fact that this is a technical solution based on the recording and processing of customers' movement patterns when the app is used. (…)"

In the Danish Data Protection Agency's view, this risk of collecting additional data via the Rejsekort app raises questions as to whether the app complies with the requirements of Article 5(1)(c) and Article 25.

On the one hand, it can be argued that the collection of personal data in the form of location data on users outside the public transport system – and thus the tracking of users' purely private movements – takes place 'automatically' if the user simply forgets to check out of the Rejsekort app. If the user has not activated the assistive features offered in the app, the collection will thus take place simply as a result of the users' passivity. This could potentially involve sensitive information, for example if, after their journey on public transport, the user visits a church, receives medical treatment, visits their trade union, etc.

Based on the information provided by Rejsekort, see section 3.3, it must be assumed that only a small proportion of users forget or fail to check out. However, as the Rejsekort system is a nationwide system accessible to the entire Danish population, it must also be assumed that there may be a non-negligible proportion of users who, over time, risk having their private movements outside public transport tracked. As long as the user does not check out, tracking may continue for several hours.

It may also be pointed out that, viewed in isolation, GPS tracking of users whilst not on public transport is not necessary for Rejsekort to provide the journey planning and ticketing service that the company is required to provide. The collection of information about the user's subsequent movements after the journey has ended is therefore irrelevant to the service that Rejsekort is required to provide.

Finally, it should be noted that the Rejsekort app's assistance features are not – and presumably cannot be – mandatory for users to opt into. According to the information provided to the Danish Data Protection Agency, activating these assistance features in the app therefore requires an active, manual opt-in on the part of users.

On the other hand, it should be noted that the collection of location data outside the public transport system only takes place when the user fails to fulfil their contractual obligation to check out at the end of their journey. It is therefore only when the user utilises the app outside its intended scope of use that additional information regarding the user's location may be collected. Rejsekort has produced comprehensive guidance material, which is available to users in a variety of formats. Users cannot therefore claim to be unaware of how the app is to be used, including the fact that they are obliged to check out at the end of their journey.

It is also worth noting that Rejsekort has built in a number of assistance features, including an option for automatic check-out, to prevent the collection of location data once a journey has ended. If users activate these features in the app, the risk of unauthorised location data being collected will be significantly reduced or eliminated.

Rejsekort has also launched other ticketing solutions in conjunction with the Rejsekort app, including a ticketing solution similar to the previous plastic Rejsekort, known as the Basiskort.

Finally, it should be noted that Rejsekort has, from the outset, been aware of the risk of users' location data being collected outside the public transport system, and that the company has implemented a number of measures to minimise this risk. This includes, amongst other things, the aforementioned assistance features, but also the fact that the app is designed in such a way that it is clear to the user on the phone's screen that the Rejsekort app (and thus GPS tracking) is activated.

Having weighed up all the above factors, which argue both for and against the Rejsekort app's compliance with the law, the Danish Data Protection Agency finds that there are not fully sufficient grounds to express criticism of Rejsekort's launch of the Rejsekort app.

As mentioned above, in this decision the Danish Data Protection Agency has considered only the design and functionality of the Rejsekort app in relation to Article 5(1)(c) and Article 25 of the General Data Protection Regulation. The Danish Data Protection Agency has therefore not, in this decision, addressed the app's compliance with other (data protection) rules.

Nor has the Danish Data Protection Agency, in this decision, taken a position on Rejsekort's communication, marketing or other aspects of the app's implementation. However, the Danish Data Protection Agency has noted that the Consumer Ombudsman, who enforces, amongst other things, the Marketing Practices Act, has addressed Rejsekort's marketing of the Rejsekort app, and that the Consumer Ombudsman has, in this connection, reported the company to the police.

The Danish Data Protection Agency's investigation into Rejsekort is hereby concluded, and the Agency will take no further action in this matter.